Smart Grid Interoperability Panel (SGIP)

Cyber Security Working Group (CSWG)

Standards Review

CSWG Standards Review Report

ANSI C12.1-2008

Code for Electricity Metering

May 10, 2011

Security Assessment of ANSI C12.1-2008: Code for Electricity Metering

1. Introduction

1.1 Correlation of Cybersecurity with Information Exchange Standards

Correlating cybersecurity with specific information exchange standards, including functional requirements standards, object modeling standards, and communication standards, is very complex. There is rarely a one-to-one correlation, with more often a one-to-many or many-to-one correspondence.

First, communication standards for the Smart Grid are designed to meet many different requirements at many different "layers" in the communications "stack" or "profile," one example of such a profile is the GridWise Architecture Council (GWAC) Stack. Some standards address the lower layers of the communications stack, such as wireless media, fiber optic cables, and power line carrier. Others address the "transport" layers for getting messages from one location to another. Still others cover the "application" layers, the semantic structures of the information as it is transmitted between software applications. In addition, there are communication standards that are strictly abstract models of information – the relationships of pieces of information with each other. Since they are abstract, cybersecurity technologies cannot be linked to them until they are translated into "bits and bytes" by mapping them to one of the semantic structures. Above the communications standards are other security standards that address business processes and the policies of the organization and regulatory authorities.

Secondly, regardless of what communications standards are used, cybersecurity must address all layers – end-to-end – from the source of the data to the ultimate destination of the data. In addition, cybersecurity must address those aspects outside of the communications system in the upper GWAC Stack layers that may just be functional requirements or may rely on procedures rather than technologies, such as authenticating the users and software applications, and screening personnel. Cybersecurity must also address how to: cope during an attack, recover from it afterwards, and create a trail of forensic information to be used in post-attack analysis.

Thirdly, the cybersecurity requirements must reflect the environment where a standard is implemented rather than the standard itself: how and where a standard is used must establish the levels and types of cybersecurity needed. Communications standards do not address the importance of specific data or how it might be used in systems; these standards only address how to exchange the data. Standards related to the upper layers of the GWAC Stack may address issues of data importance.

Fourthly, some standards do not mandate their provisions using "shall" statements, but rather use statements such as "should," "may," or "could." Some standards also define their provisions as being "normative" or "informative." Normative provisions often are expressed with "shall" statements. Various standards organizations use different terms (e.g., standard, guideline) to characterize their standards according to the kinds of statements used. If standards include security provisions, they need to be understood in the context of the "shall," "should," "may,"

and/or “could” statements, “normative,” or “informative” language with which they are expressed.

Therefore, cybersecurity must be viewed as a stack or “profile” of different security technologies and procedures, woven together to meet the security requirements of a particular implementation of a stack of policy, procedural, and communication standards designed to provide specific services. Ultimately, cybersecurity as applied to the information exchange standards should be described as profiles of technologies and procedures which can include both “power system” methods (e.g. redundant equipment, analysis of power system data, and validation of power system states) and information technology (IT) methods (e.g. encryption, role-based access control, and intrusion detection).

There also can be a relationship between certain communication standards and correlated cybersecurity technologies. For instance, if TCP/IP is being used at the transport layer and if authentication, data integrity, and/or confidentiality are important, then TLS (transport layer security) should most likely (but not absolutely) be used.

In the following discussions of information exchange standard(s) being reviewed, these caveats should be taken into account.

1.2 Correlation of Cybersecurity Requirements with Physical Security Requirements

Correlating cybersecurity requirements with specific physical security requirements is very complex since they generally address very different aspects of a system. Although both cyber and physical security requirements seek to prevent or deter deliberate or inadvertent attackers from accessing a protected facility, resource, or information, physical security solutions and procedures are vastly different from cybersecurity solutions and procedures, and involve very different expertise. Each may, in fact, be used to help protect the other, while compromises of one can definitely compromise the other.

Physical and environmental security that encompasses protection of physical assets from damage is addressed by the NISTIR 7628 only at a high level. Therefore, assessments of standards that cover these non-cyber issues must necessarily also be at a general level.

1.3 Standardization Cycles of Information Exchange Standards

Information exchange standards, regardless of the standards organization, are developed over a time period of many months by experts who are trying to meet a specific need. In most cases, these experts are expected to revisit standards every five years in order to determine if updates are needed. In particular, since cybersecurity requirements were often not included in standards in the past, existing communication standards often have no references to security except in generalities, using language such as “appropriate security technologies and procedures should be implemented.”

With the advent of the Smart Grid, cybersecurity has become increasingly important within the utility sector. However, since the development cycles of communication standards and cybersecurity standards are usually independent of each other, appropriate normative references between these two types of standards are often missing. Over time, these missing normative references can be added, as appropriate.

Since technologies (including cybersecurity technologies) are rapidly changing to meet increasing new and more powerful threats, some cybersecurity standards can be out-of-date by the time they are released. This means that some requirements in a security standard may be inadequate (due to new technology developments), while references to other security standards may be obsolete. This rapid improving of technologies and obsolescence of older technologies is impossible to avoid, but may be ameliorated by indicating minimum requirements and urging fuller compliance to new technologies as these are proven.

1.4 References and Terminology

References to the National Institute of Standards and Technology (NIST) security requirements refer to the NIST Interagency Report (IR) 7628, *Guidelines to Smart Grid Cyber Security*, Chapter 3, High-Level Security Requirements.

References to "government-approved cryptography" refer to the list of approved cryptography suites identified in Chapter 4, Cryptography and Key Management, of NISTIR 7628. Summary tables of the approved cryptography suites are provided in Chapter 4.3.2.1.

As noted, standards have different degrees for expressing requirements, and the security requirements must match these degrees. For these standards assessments, the following terminology is used to express these different degrees[1]:

- Requirements are expressed by "…shall…," which indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).
- Recommendations are expressed by "…should…," which indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).
- Permitted or allowed items are expressed by "…may…," which is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).
- Ability to carry out an action is expressed by "…can …," which is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).
- The use of the word *must* is deprecated, and should not be used in these standards to define mandatory requirements. The word *must* is only used to describe unavoidable situations (e.g. "All traffic in this lane must turn right at the next intersection.")

2. ANSI C12.1-2008 Code for Electricity Metering

2.1 Description of Document

ANSI C12.1-2008 Code for Electricity Metering establishes acceptable performance criteria for new types of ac watt-hour meters, demand meters, demand registers, pulse devices, and auxiliary

[1] The first clause of each terminology definition comes from the International Electrotechnical Commission (IEC) Annex H of Part 2 of ISO/IEC Directives. The second clause (after "which") comes from the Institute of Electrical and Electronics Engineers (IEEE) as a further amplification of the term.

devices. It describes acceptable in-service performance levels for meters and devices used in revenue metering. It also includes information on related subjects, such as recommended measurement standards, installation requirements, test methods, and test schedules. This Code for Electricity Metering is designed as a reference for those concerned with the art of electricity metering, such as utilities, manufacturers, and regulatory bodies.

Section 2 contains definitions.

Section 3, standards and standardizing equipment, outlines an appropriate chain of intermediate steps between the national standards and watt-hour meters.

Section 4 contains acceptable performance requirements of new types of electricity metering devices and associated equipment.

Section 5 contains standards for in-service performance of new metering devices.

Section 6 contains information on requirements for auxiliary pulse devices for electricity metering. The usual form of pulse initiators is that of an attachment to a meter device so arranged that the number of pulses produced is proportional to the quantity measured.

2.2 Assumptions

C12.1-2008 focuses on the design and construction of the meter, accuracy and failure handling of the meter, meter installation issues, and testing of the meter to ensure meeting the performance requirements of the electric meter. These electric meters may or may not have communications capabilities, and even if they do, those communication capabilities are not addressed in this standard.

One interpretation of the standard would be to treat all such devices as an "auxiliary device" defined in section 2.3 as: "an add-on device mounted under the meter cover that adds functionality to the meter device." Section 4.5.1 describes how and when the tests apply to auxiliary devices, Section 4.7.1 describes the test conditions for those "powered line-to-line," Section 4.7.2.5.1 describes the test for effect of voltage variation on solid-state auxiliary devices, Section 4.7.3.5.1 describes the test for effect of ambient temperature variation. However, the treatment of "auxiliary devices" is the topic of an ongoing investigation by the C12 Auxiliary Device Interest Group (AuDIG).

2.3 Assessment of Cybersecurity Content

The ANSI C12.1-2008 primarily addresses non-cyber metering issues, such as performance, measurement accuracy, installation issues, and testing. Therefore it was assessed on whether these issues could affect cybersecurity, or whether cyber attacks might affect these issues. However, since the NISTIR 7628 addresses at a high level physical and environmental security that encompasses protection of physical assets from damage, assessments of standards that cover these non-cyber issues must necessarily be at a general level.

2.3.1 Does the standard address cybersecurity? If not, should it?

This standard does not address cybersecurity and does not need to address cybersecurity since it focuses on the performance and testing of the meter. No communications or information exchanges are addressed. It does identify the need to physically seal a meter (see Sections B.12.2.5 and B.12.3.5) "*to detect unauthorized access to working parts and to electrical and magnetic devices*."

2.3.2 What aspects of cybersecurity does the standard address and how well (correctly) does it do so?

Because the standard references performance and testing requirements of electric meters without regard to any communications, the cybersecurity requirements as described in NISTIR 7628, *Guidelines to Smart Grid Cybersecurity*, are not applicable.

2.3.3 What aspects of cybersecurity does the standard not address? Which of these aspects should it address? Which should be handled by other means?

Cybersecurity is not addressed in this standard and, based on the defined scope and content of this standard, cybersecurity should not be handled within this document.

2.3.4 What work, if any, is being done currently or is planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

At this time, no work is currently proposed for the C12.1 standard.

2.3.5 Recommendations

Although basic physical security considerations have been included in the standard, such as sealing the meter against unauthorized access, it does not attempt to address the more complex cyber-physical security requirements of electric meters with sensitive and private information stored within it.

It is therefore recommended that **a standard be developed to cover the cyber-physical security requirements of electric meters,** including:

- The impact of physical tampering, physical damage, and unauthorized physical access on the security of the stored information and the communication of that information, and
- The use of physical technology, including hardware technology, to help protect cyber information, deter attackers, and/or provide information on what or how an attack was made.

2.3.6 Underwriters Laboratory (UL) addresses some of these cyber-physical issues in UL 2735: Outline of Investigation for Electric Utility Meters: "*These requirements cover electric utility meters which measure, monitor, record, transmit, or receive electrical energy generation or consumption information. Monitored parameters may include voltage, current, power, apparent power, reactive power, power factor, energy, kW-hours, varhours, and time of use*." This document could be reviewed as input to such a standard.List any references to other standards and whether they are normative or informative.

ANSI C12.1 includes only a single list of references; normative and informative references are not distinguished.

Reference	Description
ANSI/IEEE C63.4-2003	Methods of Measurement of Radio-Noise Emissions From Low-Voltage Electrical and Electronic Equipment in the Range of 9 kHz to 40 GHz
ASQ Z1.4-2003	Sampling Procedures and Tables for Inspection by Attributes

Reference	Description
ASQ Z1.9-2003	Sampling Procedures and Tables for Inspection by Variables for Percent Nonconforming
ASTM B117-2003	Standard Practice for Operating Salt Spray (Fog) Apparatus
ASTM G155 2005	Standard Practice for Operating Xenon Arc Light Apparatus for Exposure of Non-Metallic Materials Code of Federal Regulations (Telecommunication) CFR 47, Part 15—Radio Frequency Devices, Subparts A—General and B—Unintentional Radiators Chapter 13 “The Customers’ Premises, Service and Installations”, Handbook for Electricity Metering, 10th Edition, Washington, D.C.: Edison Electric Institute, 2002
IEEE 1-2000	IEEE Recommended Practice: General Principles for Temperature Limits in the Rating of Electric Equipment and for the Evaluation of Electrical Insulation
IEEE Std 100-2000	The Authoritative Dictionary of IEEE Standards Terms
IEEE C37.90.1-2002	IEEE Standard Surge Withstand Capability (SWC) Tests for Protective Relays and Relay Systems Associated with Electric Power Apparatus
IEEE C57.13-1993	IEEE Standard Requirements for Instrument Transformers
IEEE C62.41.1-2002	IEEE Guide on the Surge Environment in Low-Voltage (1000 V and less) AC Power Circuits
IEEE C62.41.2-2002	IEEE Recommended Practice on Characterization of Surges in Low-Voltage (1000 V and less) AC Power Circuits
IEC 60068-2-6 (1995)	Environmental Testing - Part 2: Tests, Test Fc: Vibration (Sinusoidal) Informative references:
IEC 60068-2-27 (1987)	Environmental Testing, Part 2: Tests, Test Ea and Guidance: Shock.
IEC 61000-4-2 (2001)	Electromagnetic Compatibility (EMC) - Part 4-2: Testing and Measurement Techniques - Electrostatic Discharge Immunity Test
IEC 61000-4-4 (2004)	Electromagnetic Compatibility (EMC), Part 4-4: Testing and Measurement Techniques - Electrical Fast Transient/Burst Immunity Test
International Safe Transit Association, Test Procedure 1A	Performance Test for Individual Packaged-Products Weighing 150 lb. (68 kg) or Less, (revision date: 2001) , Vibration and Shock
NEMA 250-2003	Enclosures for Electrical Equipment (1000 Volts Maximum)
NFPA 70-2005	National Electrical Code
UL 50-1995	UL Standard for Enclosures for Electrical Equipment